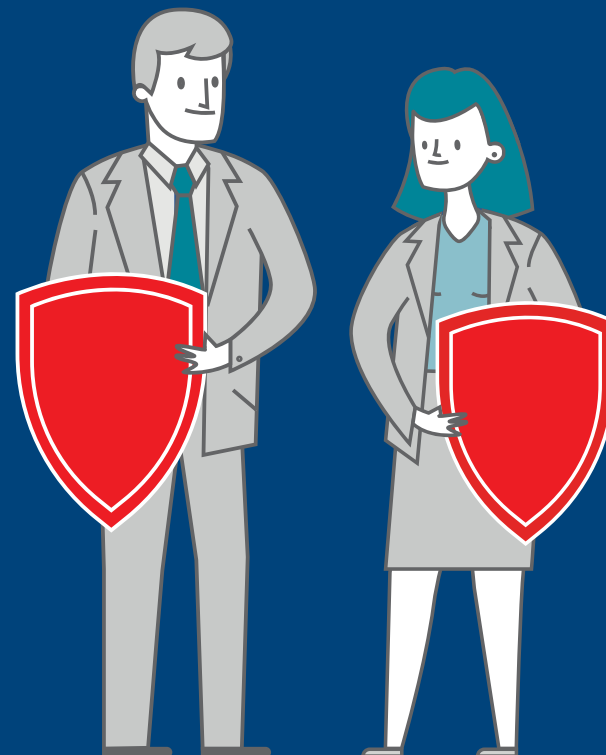


LexisNexis® Fraud Defense Network

# The Identity Fraud Prevention Playbook

*Insights and actionable recommendations  
to help protect against identity fraud*

November 2016



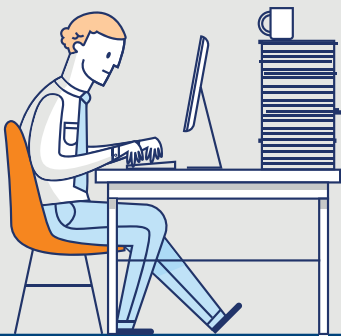
## Fraud that leverages stolen identities is not a new crime, but the digital age has enabled identity fraud at an unprecedented scale, with schemes of incredible scope and cunning.

Costs to organizations and agencies have skyrocketed into the tens of billions of dollars. In a 2016 study, 49% of fraud mitigation professionals pointed to identity fraud as the fraud scheme of greatest concern.<sup>1</sup> Aside from the significant challenges to industry, consumers are also impacted. Fraudsters stole \$15 billion from 13.1 million identity theft victims in 2015;<sup>2</sup> and the Federal Trade Commission (FTC) has ranked identity theft as the number one complaint for 15 years in a row.

In the wake of major ongoing security breaches, identities have become an easily accessible commodity allowing fraudsters to go online and purchase personally identifiable information (PII) ranging from basic name, Social Security number (SSN), address and date of birth (DOB) data, to complete social security cards, birth certificates and passports. Identity crimes involving someone's full identity are common, but a growing threat stems from synthetic identity fraud, where a new identity is manufactured from stolen bits of PII and fake identity details, making the damage to the victim's credit profile more difficult to uncover.

Traditional, stand-alone identity management and verification tools are no longer capable of delivering efficient identity proofing while simultaneously fending off the onslaught of highly sophisticated fraud methods.

**This playbook outlines some of the common identity fraud schemes within four different industry sectors and government, along with recommended ways for organizations and agencies to address the growing problem.**



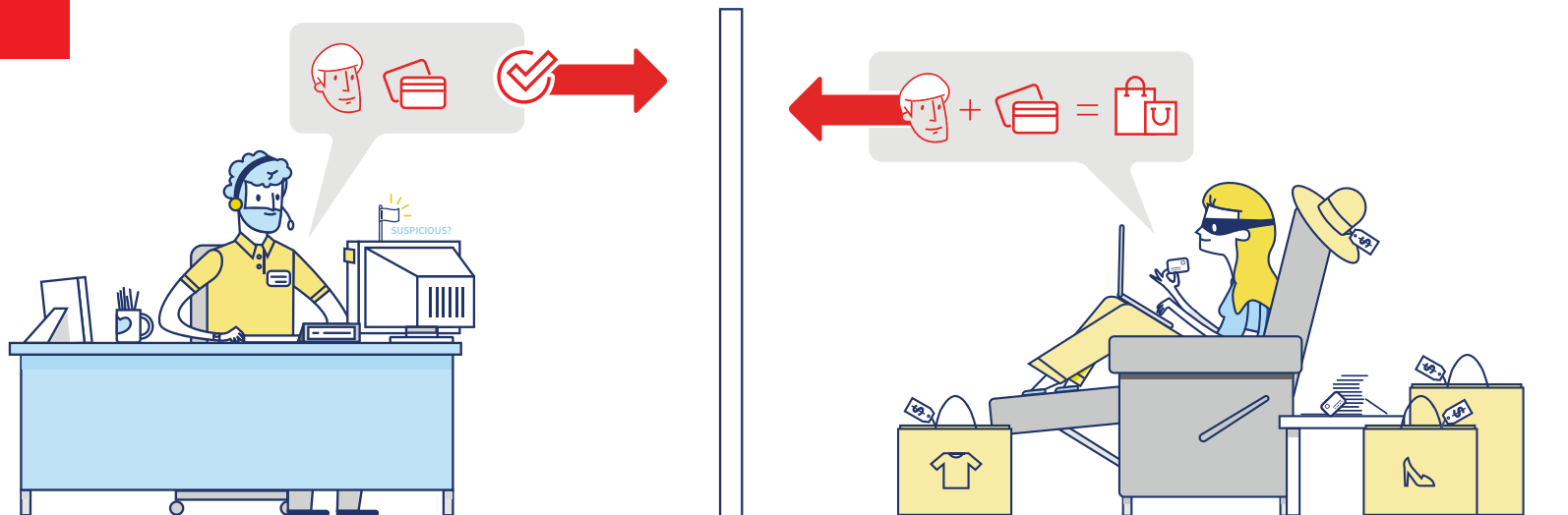
<sup>1</sup> LexisNexis, 2016 Fraud Mitigation Study, <http://www.lexisnexis.com/risk/insights/cross-industry-fraud.aspx>

<sup>2</sup> Javelin, 2016 Identity Fraud Report, <https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point>

## Table of Contents

Financial Services Fraud .....	1-2
Retail Fraud .....	3-4
Property & Casualty Insurance Fraud .....	5-6
Health Care Identity Fraud .....	7-8
Government Fraud Resulting from Stolen Identities .....	9
Tax Refund Fraud .....	10-11
Public Assistance Fraud .....	12-13
Resources .....	14

THE FRAUDSTER'S PLAY



FINANCIAL SERVICES FRAUD

Identity fraud in the financial services industry may involve credit cards, loans, checking accounts, debit cards, mortgages and other financial services products.

Financial services fraud is primarily perpetrated by one of two methods: 1) new account or application fraud, where a thief uses stolen identity information or a synthetic identity to fraudulently open an account and then defaults on obligations, or 2) account takeover fraud, when a fraudster impersonates a real customer to take control of an account and make unauthorized transactions. New application and account takeover fraud each account for 20 percent of all fraud losses within the financial services industry.<sup>1</sup>

Financial fraud using false identity information more than doubled in 2015, with 1.5 million consumers impacted for a total cost of \$15 billion.<sup>2</sup> This number is expected to grow even more now that the industry is transitioning to Europay, MasterCard and Visa (EMV) technology. The chips in EMV credit cards make it more difficult for fraudsters to produce counterfeit cards, so they have migrated to identity theft-related crimes that tend to have bigger returns. Unfortunately, identity-related fraud is difficult for institutions to detect, and may be written off as a credit risk until a customer realizes what has happened.

<sup>1</sup> LexisNexis, 2016 Card Issuer Fraud Study, "Issuers Confront Application Fraud and Account Takeover in a Post-EMV U.S."






<sup>2</sup> Javelin, 2015 Strategy & Research Report



FRAUD AND TECHNOLOGY

Today's identity fraudsters leverage the Internet. One hundred years ago, they used the phone. In the early 20th century, perpetrators assumed the identity of another person, and then called a bank to request a wire transfer from the victim's account.

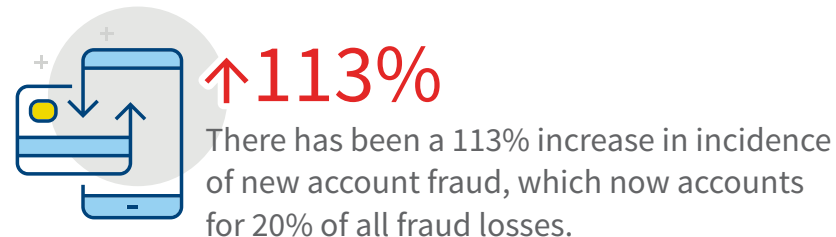
## THE AGENCY'S BEST DEFENSE METHODS

-  Incorporate identity fraud detection tools during account opening processes that include the following:
  - Device fingerprinting that reviews key variables in the device submitting an online application (and the software running on that device) to ensure that it reflects the information contained in the application
  - Sophisticated identity fraud risk scoring and rules-based processes designed to flag the highest risk applications
-  Use hot lists that compile the relevant data of past frauds and suspicious or high-risk activity, store this information for future review, and integrate it into monitoring activities
-  Consider knowledge-based authentication (KBA) “out-of-wallet” questions to the applicant
-  Monitor accounts for high-risk transactions or session activity—even accounts where a prior relationship exists or with a window period—as fraudsters can predict when the window timeframes expire and create sleeper accounts that become active
-  Implement audits, internal processes and training that educate employees about the need to safeguard personally identifiable information (PII)

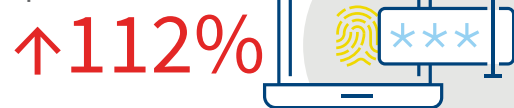
“As fraudsters will continue to evolve with technology, it is important for anti-fraud professionals to stay on top of the current trends in order to prevent fraud before it’s able to occur.”

*James D. Ratley, President  
Association of Certified Fraud Examiners*

### 2015 DEBIT FRAUD BENCHMARK STUDY

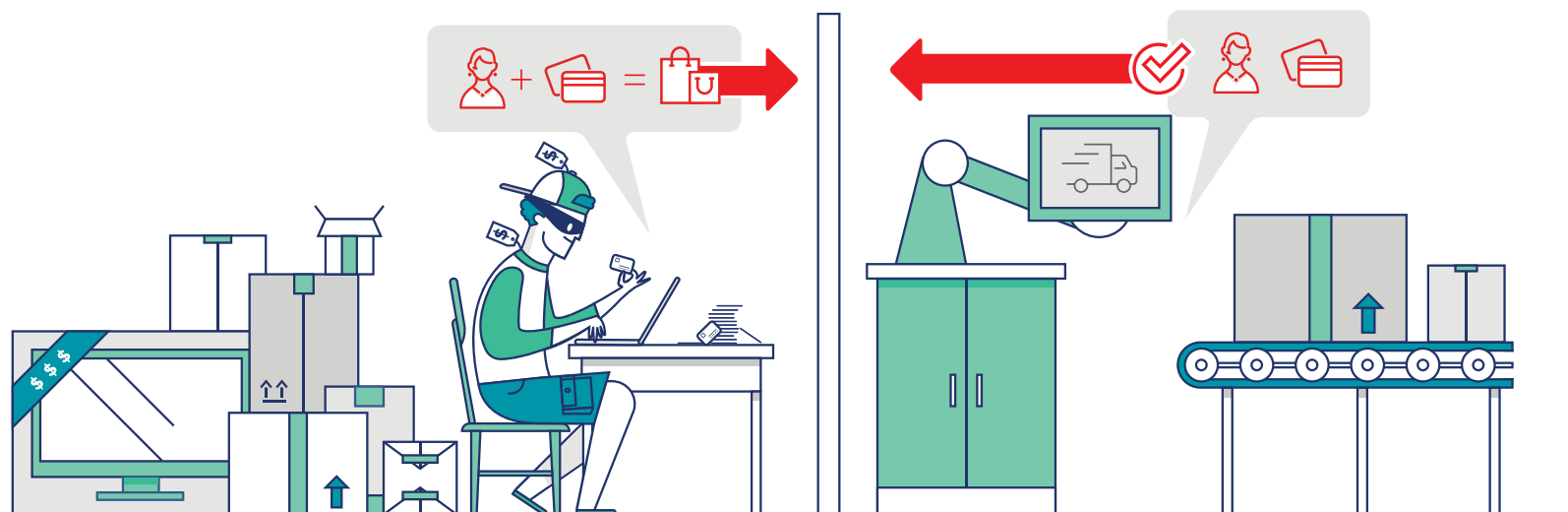


Incidents of account takeover jumped 112% in the first quarter of 2015 compared to the same time period in 2014.



Source: Auriemma Consulting Group, 2015 Debit Fraud Benchmark Study,  
<http://www.acg.net/debit-card-account-takeover-and-online-fraud-side-effects-of-emv-on-the-rise/>

## THE FRAUDSTER'S PLAY

**RETAIL FRAUD**

Estimates suggest e-commerce will top \$500 billion by 2020<sup>1</sup>, and as more retail transactions become virtual, fraudsters are adapting to the times, moving from in-store fraud primarily involving stolen or counterfeit credit cards to new methods associated with anonymous e-payment and Card-Not-Present (CNP) transactions that often leverage stolen or synthetic identities.

Larger remote channel merchants, in particular, are impacted, as evidenced by several recent high-profile security breaches involving well-known retail brands. Tricky criminals might also take advantage of retailers that allow returns to be made in store—especially where identification is not required during the return.

Regardless of whether the transaction occurs remotely or in-store, the challenge for retailers will be to effectively identify fraudulent transactions and fast-track the legitimate ones without creating undue friction for customers.

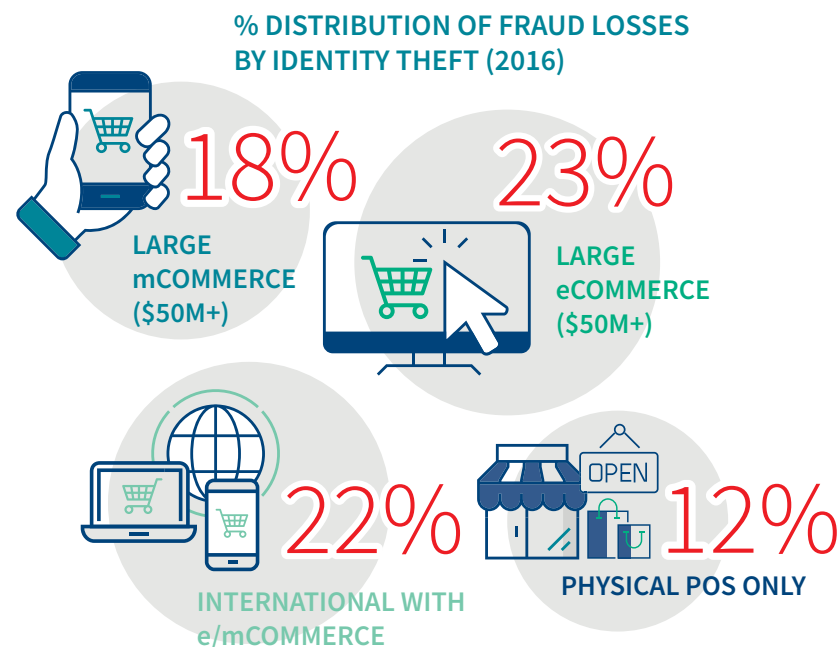
<sup>1</sup> Forrester Research 2015 Web-Influenced Sales Forecast, 2015-2020, <https://www.internetretailer.com/2016/01/29/online-sales-will-reach-523-billion-2020-us>

## THE AGENCY'S BEST DEFENSE METHODS

- ✔ Integrate fraud management into risk assessment workflow
- ✔ Automate identity validation and authentication using knowledge-based quizzes and other tools prior to a transaction
- ✔ Implement processes and consider investing more in systems that automatically flag suspicious transactions, and combine them with multiple fraud mitigation solutions that recognize anomalies that suggest errors or point to intentionally falsified identity data
- ✔ When conducting manual reviews use the best tools with the most complete and accurate information available
- ✔ Dynamically adjust security level to suit scenario to achieve an appropriate balance in transaction friction and customer transaction experience
- ✔ Consider all forms of payment and transactions in risk scenario evaluations, including gift cards and reward programs, as anything that can be converted to something of value may be subject to attacks
- ✔ Receive real-time pass/fail results and integrate monitoring with cybersecurity detection and threat analysis
- ✔ Consider external intelligence and information sources beyond internal detection capabilities to expand visibility of criminal activities and methods

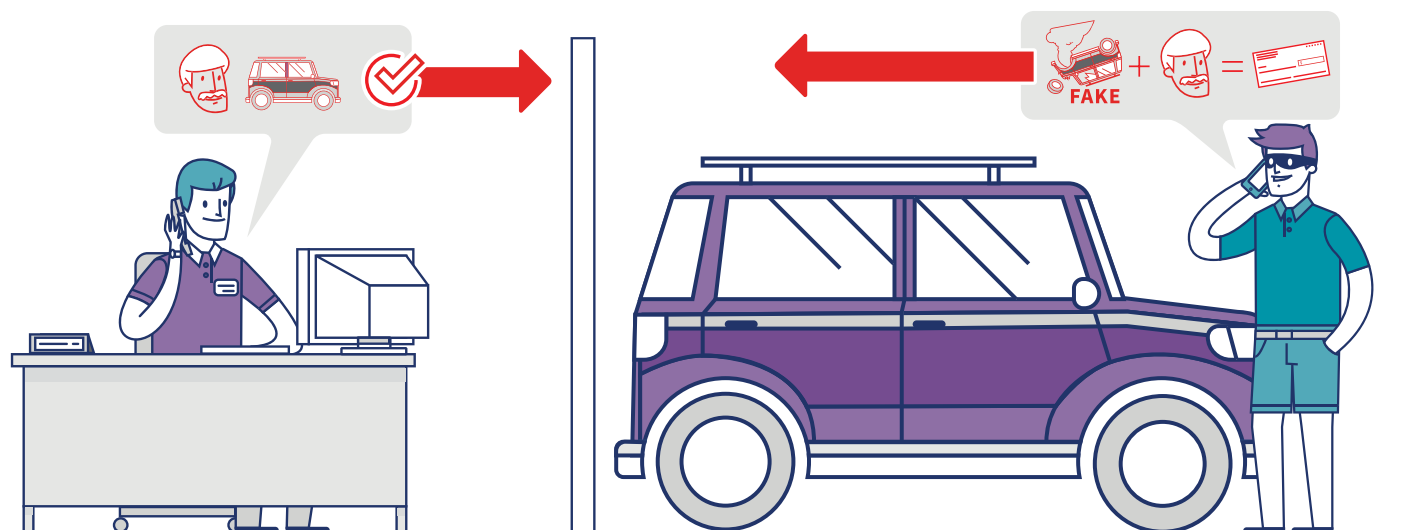
“Adversaries have evolved into interconnected, highly functional criminal rings. These rings are working in unison to leverage their specialized skills in all stages of information theft from cybersecurity breach to monetization through fraud. To combat these threats, a collaboration within cybersecurity and fraud prevention functions internal to organizations and across industries is critical.”

*Brian Engle, Executive Director  
Retail Cyber Intelligence Sharing Center*



Source: LexisNexis® 2016 True Cost of Fraud<sup>SM</sup> Study

## THE FRAUDSTER'S PLAY



## PROPERTY &amp; CASUALTY INSURANCE FRAUD

Property and Casualty insurance fraud is an expensive problem, with estimates at \$32 billion annually.<sup>1</sup> It is not clear how much of this stems from identity-related types of crimes, but the potential is increasing as the insurance industry has moved away from in-person interaction toward online services and a direct sales model. Nearly three quarters of auto insurance shoppers in 2015 obtained a quote online,<sup>2</sup> with other insurance lines beginning to follow suit.<sup>3</sup>

Identity-related fraud schemes are often perpetrated when organized crime rings use stolen or synthetic identities to file fraudulent claims and then cash the insurance checks. In a common spin on identity fraud, unscrupulous individuals may apply for insurance as themselves, but purposely misrepresent certain identity details to receive lower rates (example: car owners in a high premium geographical area represent that they live in another location to receive lower rates, or companies that misrepresent the number or job descriptions of employees to avoid paying workers' compensation insurance). In other schemes, thieves use stolen personal information to impersonate an insurance agent then submit applications for life insurance using false or stolen identity information so that they can collect a commission on the new policies.

<sup>1</sup> Insurance Institute, August 2016, <http://www.iii.org/issue-update/insurance-fraud>

<sup>2</sup> J.D. Power, 2016 U.S. Insurance Shopping Study,<sup>SM</sup> April 2016, <http://www.jdpower.com/resource/jd-power-us-insurance-shopping-study>

<sup>3</sup> McKinsey & Company, 2011 "The Multichannel Imperative for Property and Casualty Carriers in Personal Lines."



## THE AGENCY’S BEST DEFENSE METHODS

✔ Use mobile device technology and capabilities, data and advanced analytics and linking tools that can quickly verify and confirm valid identities and recognize anomalies through driver’s license bar code imagery. Utilizing mobile device technology thwarts fraud without adding friction to the policy application workflow

✔ Leverage external data sets to gain a multi-dimensional view of the applicant and reduce dependence on self-reported information that may be false or inaccurate. Sources include:

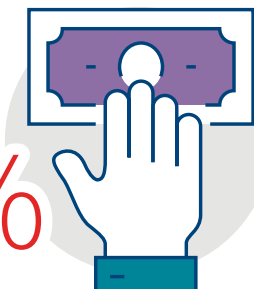
- Shared data from other industries that is not claims data, but that may shed light on your investigation
- Public records data—Identification data including name, phone number, address and SSN, as well as other “footprint” data, like bankruptcies, deceased files, watch lists and criminal records

“The exploiting of stolen and synthetic identities is embedded in property-casualty insurance. The rapid growth of online coverage is one emerging new field of vulnerability. Insurers must firm up their defenses against identity threats, to protect their bottom lines and ensure honest policyholders the safest insurance experience possible.”

*Dennis Jay, Executive Director  
Coalition Against Insurance Fraud*

The National Insurance Crime Bureau estimates fraud is involved in approximately

**10%**



...costing policy holders an estimated

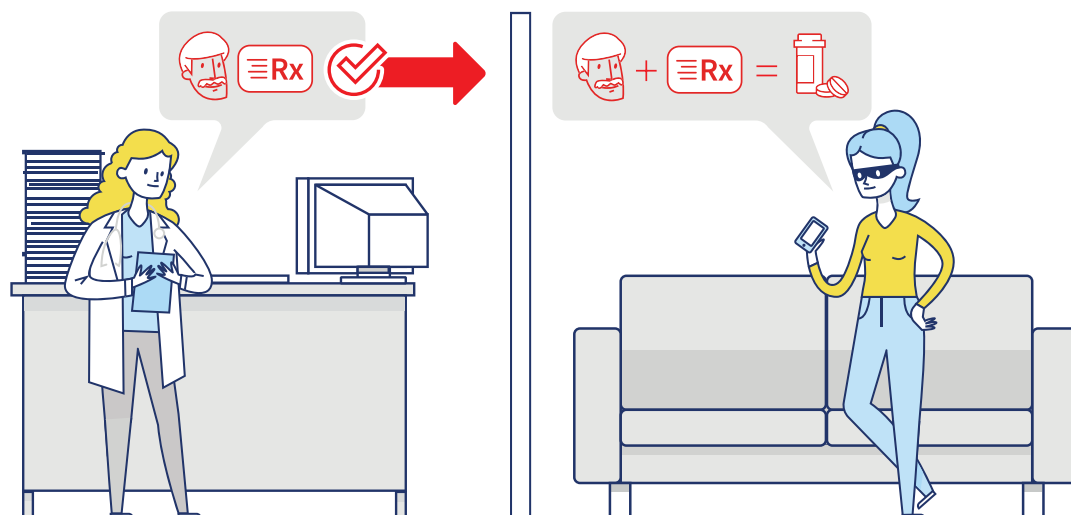
**\$200-\$300**

a year in added premiums.

**No line of insurance—from Home and Auto to Life and Commercial—is immune.**

Source: Insurance Industry studies, as published on <http://InsuranceFraud.org>

## THE FRAUDSTER'S PLAY



## HEALTH CARE FRAUD IMPACTING PAYERS &amp; PATIENTS

Identity fraud in health care is on the rise. The Affordable Care Act of 2010 is introducing millions of new patients into the health care system,<sup>1</sup> and more patients bring more opportunities for fraud—including additional chances for newly insured individuals' identities to be stolen, or for applicants to game the system using false identity information.

The problem is compounded with the increasing virtualization of the industry. Online portals and increasing telemedicine encounters enable patients to sign up, coordinate, receive and review care activity without being physically present in a provider's office, making it that much more critical to have appropriate safeguards in place. Without them, payers risk potentially millions of dollars in fraud losses, and patients risk their health—or even their lives—if identity details are botched and the wrong treatment is administered.

## PROVIDER FRAUD

Fraudulent health care providers employ many sneaky tactics to create confusion around identities and the claims associated with them, including creating fake identities or even using the identities of deceased individuals to submit fraudulent claims. Verifying and resolving identities can even be challenging when dealing with legitimate providers that may work in multiple locations and use multiple sets of contact information.

<sup>1</sup> U.S. Department of Health and Human Services, 2016 Health Insurance Coverage and the Affordable Care Act, <http://www.hhs.gov/about/news/2016/03/03/20-million-people-have-gained-health-insurance-coverage-because-affordable-care-act-new-estimates>

## THE AGENCY’S BEST DEFENSE METHODS

### FOR PAYERS & PATIENTS

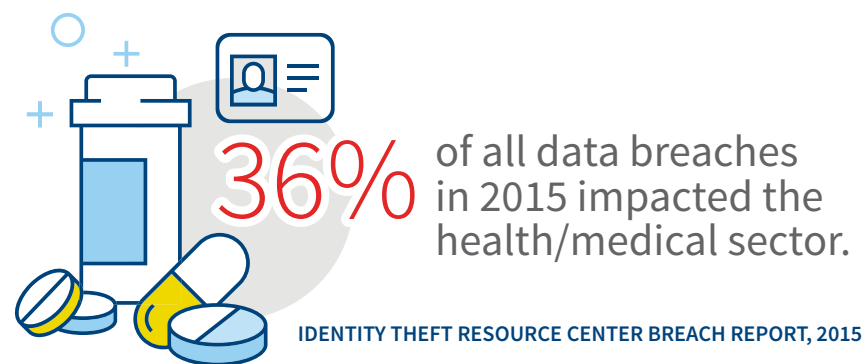
- ✓ Investment in technologies that help aggregate and join single patient information coming in from multiple sources
- ✓ Big Data and advanced analytics to uncover schemes and shady business relationships, and better understand connections between patients, doctors, facilities and other care givers

### FOR FRAUDULENT PROVIDERS

- ✓ Move from claim-level fraud prevention strategies to provider-level strategies using data, advanced analytics and linking tools that can quickly verify and confirm valid provider identities and recognize anomalies that suggest errors or intentionally falsified identity data
- ✓ Gather data from multiple sources, including:
  - Intra-industry contributory data—Claims data shared by many payers to compile the industry’s contributory database
  - Shared data from other industries that is not claims data, but that may shed light on your investigation
  - Public records data—Identification data including name, phone number, address and SSN, as well as other “footprint” data, like bankruptcies, deceased files, watch lists and criminal records

“We know that the old way of fighting fraud, where public and private payers stay narrowly focused on their individual datasets, isn’t the most effective strategy. Doing so only provides a narrow snapshot of the fraud; what is needed to combat the full scope of the problem is a broader view of how it is happening.”

*Louis Soccoccio, CEO  
National Health Care AntiFraud Association*



## GOVERNMENT SECTOR

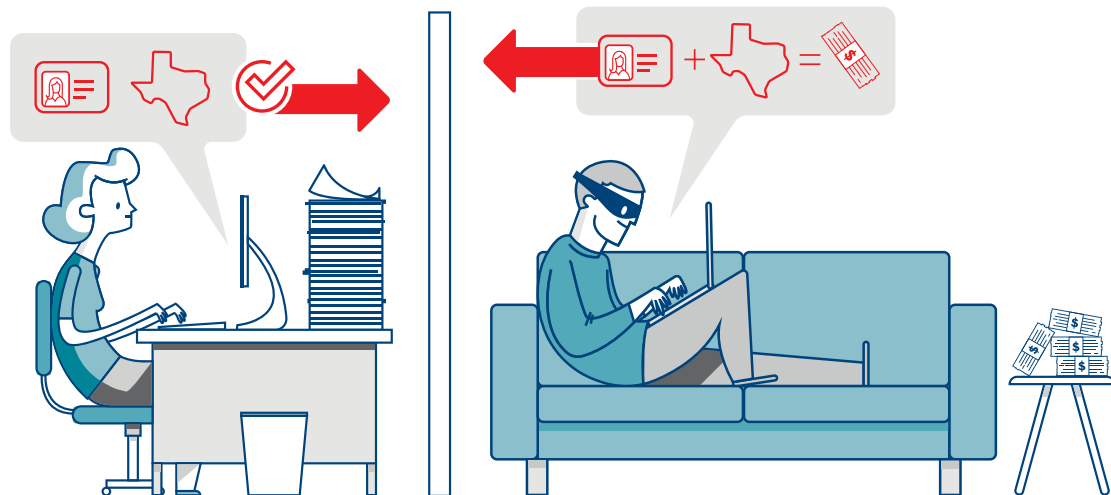
## The impact of identity theft on the government sector reaches far and wide, costing Americans tens of billions of dollars every year.

No agency is safe, with thieves targeting the federal and state income tax systems, state and federal benefits programs like Medicaid, the Supplemental Nutrition Assistance Program (SNAP) and Temporary Assistance for Needy Families (TANF); and other programs developed to help citizens or government recipients in need, like unemployment insurance, Public Housing/Section 8 benefits, the federal student loan program, and even businesses and their owners. These thieves come in a range of forms, from lone wolf fraudsters to highly-organized domestic and international crime rings.

The shift toward identity fraud crimes against government agencies in recent years may be attributed to the move from “in line” service at brick-and-mortar agency offices toward online services that make identity authentication more challenging. Agencies additionally have adopted traditional data protection approaches that make it easy for criminals but hard for government to protect us. Finally, with more than 2,000 federal agencies and departments plus their state and local counterparts, the sheer size and complexity of the government makes it an easy target for fraudsters.

Collectively, these and other factors contribute to the substantial impact of identity fraud on the government sector. According to the Federal Trade Commission (FTC), half of all reported identity theft incidents in 2015 pertained to **government documents and benefits**, and most of those were related to **tax and revenue**. The following sections examine these two most prevalent types of identity-related government fraud.

THE FRAUDSTER'S PLAY



TAX REFUND FRAUD

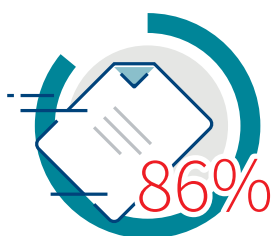
Identity-based income tax fraud is perpetuated when criminals either use stolen personal identification information (PII) to file another taxpayer’s return, or file fraudulent returns by using a synthetic identity manufactured from bits of PII from multiple taxpayers.

These types of crimes have increased significantly, and particularly at the state level—in some states by as much as 3,700%.<sup>1</sup> The troubling trend is also illustrated by the fact that income tax-related identity theft has consistently been one of the top consumer complaints to the Federal Trade Commission (FTC) in recent years, and continues to grow in numbers, increasing from 32.8% in 2014 to 45.3% in 2015.<sup>2</sup>

Increases can be explained by tax payer schemes that include filing a state return separately from the federal return, where the unlinked forms make identity fraud more difficult to uncover. In addition, states are increasingly migrating to online filing processes but are limited in their ability to verify that the individual filing and requesting a refund is in fact the real individual entitled to the refund.

<sup>1</sup> Krebs on Security, The Rise in State Tax Refund Fraud, February 2015

<sup>2</sup> Federal Trade Commission, February 2016 “Consumer Sentinel Network Data Book, January to December 2015,” <http://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2015>









WHAT THE TAX MAN SAID

86% of state government tax administration officials view identity fraud as a **major problem** within the state refund process.

Source: 2015 State Income Tax Refund Identity Fraud: Governing Institute and LexisNexis Research Report, June 2015

## THE AGENCY’S BEST DEFENSE METHODS

-  Systems and tools that help with identity verification including integrated tax systems, or systems designed to identify tax returns with significant signs of negligence or identity fraud; such as automated reviews within the integrated tax system
-  Analytics to filter and extract information
-  Processes that review and validate each refund request before issuance
-  Cross-matching that leverages external databases like the Social Security Administration Death Master File & Index, third-party public records databases with identity-based filters, the Internal Revenue Service, state and local police departments and the United States Postal Service
-  Sharing best practices. Some states are more advanced in combatting the identity theft tax fraud problem, and agencies can learn from each other
-  Analyzing identities beyond the tax system, including contributory databases or networks that house details about stolen identities to be accessed by all participants

“At the Identity Theft Resource Center we have consistently seen a significant percentage in tax return fraud victims each year. It’s absolutely crucial the government continues to review all options to help reduce and lessen the impact on individuals; we need continued discussions about best practices for entities that collect and store data, and it’s essential we arm consumers with the information they need so they can do their part in combating this crime.”

*Eva Velasquez, President/CEO  
Identity Theft Resource Center*



### DID YOU KNOW

Hilda Schrader Witcher became the **first identity theft victim** in 1938 when her actual Social Security Number was printed on “demo” cards included in the display pockets of wallets sold by a wallet manufacturer. This caused confused customers to use Hilda’s Social Security number as their own.

Source: Biegelman, Martin T. Identity Theft Handbook: Detection, Prevention, and Security. Hoboken, N.J.: John Wiley and Sons, Inc., 2009, p.14

**THE FRAUDSTER'S PLAY**



**PUBLIC ASSISTANCE FRAUD**

Over the past decade, government programs have become highly vulnerable to fraud, a good portion of which stems from identity theft.

Government agencies have moved toward offering more online services. The virtual process offers a new layer of convenience for applicants, but also carries new risks because the vast amounts of documentation and in-person appointments that were previous deterrents to potential fraudsters are no longer required. Other contributing factors to the identity fraud problem include the large number of government agencies, making it easy for fraudsters to exploit multiple agencies without being caught. Criminals can also tackle local, state and federal authorities simultaneously, often using the same stolen identities over and over again.

What's more, many government programs evolved before Internet fraud became pervasive, and these organizations now find themselves ill-equipped to mitigate today's unprecedented levels of fraud. Agencies rarely share real-time information across government boundaries and often lack access to other public but non-governmental sources.

Failure to detect fraud immediately can result in a chain reaction of costly improper payments and time wasted on deceitful, non-qualified beneficiaries. But the most disturbing impact may be when criminals wrongfully claim public assistance benefits in the name of deserving individuals.





**A FEDERAL OFFENSE**


Identity theft was designated a federal crime in 1998 via the Identity Theft Assumption Deterrence Act (P.L. 105-318).

Source: S.R. 105-274. The Identity Theft and Assumption Deterrence Act of 1998, S 512, HR 1813, 105th Cong., 2nd session, Congressional Record 144, Issue 139: H9993-9998, <http://www.gpo.gov/fdsys/pkg/CREC-1998-10-07/pdf/CREC-1998-10-07-senate.pdf>

## THE AGENCY'S BEST DEFENSE METHODS

- 

Combine data through a centralized hub or contributory database. Reduce fraud by identifying individuals who are seeking benefits from agencies multiple times within and across state lines. This type of approach can focus on one type of program such as SNAP or expand coverage across multiple government programs
- 

Evolve from rules-based systems to identity-based systems that apply multi-factor authentication using a layered approach to determine if the identity exists and if it actually belongs to that person
- 

Leverage external data sets to gain a multi-dimensional view of the applicant through identity intelligence and reduce dependence on self-reported information that may be false or inaccurate

The federal government conservatively estimates that billions of dollars annually are spent on improper payments, which include identity theft.



**\$17.5 billion**

**MEDICAID** 6.7% improper payment rate

**\$5.6 billion**

**UNEMPLOYMENT INSURANCE**

11.6% improper payment rate

**\$2.4 billion**

**SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM (SNAP)**

2.4% improper payment rate

Other assistance programs have similar improper payment rates.

Source: [paymentaccuracy.gov](http://paymentaccuracy.gov), a website of the U.S. Department of the Treasury, in coordination with the U.S. Department of Justice and Office of Management and Budget.



## RESOURCES

### Association of Certified Fraud Examiners (ACFE)

The Association of Certified Fraud Examiners (ACFE) is the world's largest anti-fraud organization and premier provider of anti-fraud training and education. Together with nearly 80,000 members, the ACFE is reducing business fraud worldwide and inspiring public confidence in the integrity and objectivity within the profession. For more information, visit [ACFE.com](http://www.acfe.com).

The Association of Certified Fraud Examiners presents the 2016 ACFE Report to the Nations on Occupational Fraud and Abuse as an essential tool for all those in the anti-fraud profession. The report provides an analysis of 2,410 cases of occupational fraud that occurred in 114 countries throughout the world.

<http://www.acfe.com/rttt2016.aspx>

### Coalition Against Insurance Fraud (CAIF)

The Coalition Against Insurance Fraud is America's only anti-fraud alliance speaking for consumers, insurance companies, government agencies and others.

Through its unique work, the Coalition empowers consumers to fight back, helps fraud fighters better detect this crime and deters more people from committing fraud.

The Coalition supports this mission with a large and continually expanding armory of practical tools: Information, research & data, services and insight as a leading voice of the anti-fraud community.

<http://www.insurancefraud.org/statistics.htm#4>

### Identity Theft Resource Center (ITRC)

The ITRC provides no cost victim assistance and consumer education through its call center, website, social media channels, live chat feature and ID Theft Help Mobile App. For more information, visit <http://www.idtheftcenter.org>

Read the [Aftermath Report](#), view a [video tip](#) on how to protect your identity and get more [insights about government identity theft](#).

### LexisNexis® Fraud Defense Network

The LexisNexis® Fraud Defense Network connects professionals and organizations from financial services, insurance, retail, government, and health care with best practices, resources and innovative fraud prevention tools, including a comprehensive cross-industry fraud database. For more information, visit <http://www.lexisnexis.com/risk/fraud-defense-network/>

<http://www.lexisnexis.com/risk/insights/fraud-defense-shared-data.aspx>

<http://www.lexisnexis.com/risk/downloads/whitepaper/2016-LexisNexis-Fraud-Mitigation-Study.pdf>

### The National Health Care Anti-Fraud Association (NHCAA)

Founded in 1985, the National Health Care Anti-Fraud Association (NHCAA) is the leading national organization focused exclusively on the fight against health care fraud. We are and have always been a private-public partnership - our members comprise nearly 90 private health insurers and those public-sector law enforcement and regulatory agencies having jurisdiction over health care fraud committed against both private payers and public programs.

The Anti-Fraud Management Survey is NHCAA's benchmarking tool with which member organizations can compare a wide variety of aspects of their respective anti-fraud operations against those of the field in general. The Executive Summary offers unique insight into the anti-fraud efforts of our nation's health insurers.

[https://www.nhcaa.org/media/104750/2015\\_mgmtsurvey\\_executivesummary.pdf](https://www.nhcaa.org/media/104750/2015_mgmtsurvey_executivesummary.pdf)

### Retail Cyber Intelligence Sharing Center (R-CISC)

The Retail Cyber Intelligence Sharing Center (R-CISC) is the single most trusted cybersecurity community for retail with the combined power of worldwide leading brands combatting consumer threats. We know retail cybersecurity, we are the R-CISC, and we are stronger together. To learn more about how R-CISC members gain insight and intelligence, visit us at <http://r-cisc.org>.

The Retail Cyber Intelligence Sharing Center (R-CISC) invites all retailers, online retailers, restaurants, hotels, grocery stores and other consumer facing organizations to visit <https://r-cisc.org/2016/10/18/r-cisc-fraud/> for additional strategies to combat the rising tide of fraudulent transactions and credit card chargebacks, identity theft, account takeover, and other top problems that R-CISC members are solving through information sharing.